**Informe Técnico**

**Cross-Site Scripting (XSS) en Campo de Comentarios de Aplicación Web**

**1. Título del Hallazgo**

**Vulnerabilidad de Cross-Site Scripting (XSS) Reflejado en Módulo de Comentarios**

**2. Descripción**

Durante una prueba de seguridad controlada en la aplicación web objetivo, se identificó una vulnerabilidad de **Cross-Site Scripting (XSS)** en el campo de comentarios. La aplicación no valida ni sanitiza adecuadamente los datos ingresados por el usuario antes de mostrarlos en la interfaz, lo que permite la inyección de código JavaScript malicioso. Esta vulnerabilidad fue detectada mediante análisis manual con apoyo de un proxy interceptador (**Burp Suite**).

**3. Evidencia Técnica**

* **Payload utilizado:**
* <script>alert("XSS")</script>
* **Comportamiento observado:** Al ingresar el payload en el campo de comentarios y publicarlo, el navegador ejecutó un cuadro de alerta con el mensaje "XSS".
* **Reproducción paso a paso:**
  1. Acceder al módulo de comentarios de la aplicación.
  2. Insertar el payload en el campo de texto.
  3. Enviar el formulario.
  4. Observar que el comentario se refleja sin sanitización, ejecutando el código JavaScript.

**4. Evaluación de Impacto y Riesgo**

* **Severidad estimada (CVSS v3.1):** 6.1 (Medium) – vector de ataque en cliente, explotación sencilla.
* **Activos en riesgo:**
  + Sesiones de usuarios autenticados (robo de cookies).
  + Integridad de la aplicación (modificación de contenido mostrado).
  + Confidencialidad de datos sensibles (exfiltración de información).
* **Clasificación de riesgo:** **Alto** en contexto productivo, debido a su potencial de robo de sesiones e inyección de contenido malicioso.

**5. Recomendaciones Técnicas**

1. Implementar **sanitización y validación de entradas** en el servidor, rechazando etiquetas <script> y caracteres especiales.
2. Escapar salidas en HTML para que el navegador interprete el texto como contenido y no como código.
3. Configurar **Content Security Policy (CSP)** para limitar la ejecución de scripts no autorizados.
4. Implementar filtros de seguridad en WAF (Web Application Firewall) como medida complementaria.

**6. Referencias**

* OWASP Top 10 – A03:2021 Injection
* OWASP Cheat Sheet – XSS Prevention

**7. Reflexión Final**

Un informe profesional de vulnerabilidades se diferencia de una simple alerta técnica porque **estructura la información en secciones claras** (evidencia, impacto, mitigación), facilitando la comprensión tanto al equipo técnico como a la gerencia. Este ejercicio reforzó la importancia de un lenguaje formal y orientado a la acción, donde cada hallazgo no solo se documenta, sino que se contextualiza en términos de **riesgo y soluciones prácticas**, garantizando que el reporte sea útil para la toma de decisiones estratégicas en ciberseguridad.